United States District Court

EASTERN DISTRICT OF NEW YORK

In the Matter of the Search of

THE PREMISES KNOWN AND DESCRIBED AS THE FIRST FLOOR OF 137-07 FRANKTON STREET, ROSEDALE, NEW YORK 11422

SEARCH WARRANT
CASE NUMBER:

TO: Special Agent Cordel James and any Authorized Officer of the United States

Affidavit(s) having been made before me by Special Agent Cordel James (Affiant) who has reason to believe that ☐ on the person of ☑ on the premises known as

THE FIRST FLOOR OF 137-07 FRANKTON STREET, ROSEDALE, NEW YORK 11422

(The PREMISES is a two story multiple family house, with a basement. The first floor is made out of a brown brick; the second floor has green shingles. The house has multiple windows. There is a driveway that runs from the street, along the side of the house, to the back yard. There is no garage. There are two front doors made of a solid light wood, with black trim. The number "137" appears between the two doors, with "07" below it. There is a pathway which leads to stairs to the front door.)

in the EASTERN District of NEW YORK there is now concealed a certain person or property, namely (describe the person or property) See Attachment

I am satisfied that the affidavit(s) and any recorded testimony establish probable cause to believe that the person or property so described is now concealed on the person or premises above-described and establish grounds for the issuance of this warrant.

YOU ARE HEREBY COMMANDED to search on or before July 8, 2007 (Date)
(not to exceed 10 days) the person or place named above for the person or property specified, serving this warrant and making the search in the daytime - 6:00 A.M. to 10:00 P.M. and if the person or property be found there to seize same, leaving a copy of this warrant and receipt for the person or property taken, and prepare a written inventory of the person or property seized and promptly return this warrant to DUTY MAGISTRATE (United States Judge or Magistrate) As required by law.

June 28, 2007 at 6:37 PM
Date and Time Issued

at Brooklyn, New York
City and State

Honorable Marilyn D. Go, Magistrate Judge, EDNY
Name and Title of Judicial Officer

Signature of Judicial Officer

02227

ATTACHMENT A

PROPERTY TO BE LOCATED AND SEIZED WITHIN THE PREMISES KNOWN AND DESCRIBED AS AT 137-07 FRANKTON STREET, ROSEDALE, NEW YORK 11422

a. The three computers, a scanner printer and two laptops identified as follows:

i. an HP Computer Pavillion with Serial Number MXX7130852;

ii. an HP Office Jet Pro Scanner Printer with Serial Number MY71B20M9;

iii. In a bedroom in the back of the house, where CLAUDIA FRANCIS was sleeping there was an HP Pavilion Laptop with Serial Number 2CD712251R;

iv. In a room that appeared to be that of CLAUDIA FRANCIS' sons, there were: (i) a Compaq Laptop Serial Number 1V1BKDKN3648; (ii) a Compaq Presario Computer with Serial Number CNC33909V3;

v. In a room that appeared to be that of CLAUDIA FRANCIS' daughter, there was a Compaq Presario Computer with Serial Number MXQ033813Z1.

b. The two safes, one a Century 1100 Model and one a Century 1330 model, and the contents thereof after opening;

c. The televisions and other electronic equipment such as DVD recorders, printers, camcorders, Playstation, X-box 360 and videos.

d. Computer hardware, meaning any and all computer equipment including all electronic devices which are capable of collecting, analyzing, creating, displaying, converting, storing, concealing, or transmitting electronic, magnetic, optical, or similar computer impulses or data. Included within the definition of computer hardware is any data processing hardware (such as central processing units and self-contained laptops or notebook computers), internal or peripheral storage

devices (such as fixed disks, external hard disks, floppy disk drives, and diskettes, tape drives and tapes, optical and compact disk storage devices, and other memory storage devices); peripheral input/output devices (such as keyboards, printers, scanners, plotters, video display monitors, and optical readers); related communications devices (such as modems, cables and connections, recording equipment, RAM and ROM units, acoustic couplers, automatic dialers, speed dialers, programmable telephone dialing or signaling devices, and electronic tone generating devices); and any devices, mechanisms, or parts that can be used to restrict access to such hardware (such as physical keys and locks);

e. Computer software, meaning any and all information, instructions, programs, or program codes, stored in the form of electronic, magnetic, optical, or other media, which is capable of being interpreted by a computer or its related components. Computer software may also include data, data fragments, or control characters integral to the operation of computer software, such as operating systems software, applications software, utility programs, compilers, interpreters, communications software, and other programming used or intended to be used to communicate with computer components.

f. Computer-related documentation, meaning any written, recorded, printed, or electronically-stored material which explains or illustrates the configuration or use of any seized computer hardware, software, or related items.

g. Computer passwords and data security devices, meaning any devices, programs, or date - whether themselves in the nature of hardware or software - that can be used or are designed to be used to restrict access to, or to facilitate concealment of, any computer hardware, computer software, computer-related documentation, or electronic data records. Such items include, without limitation, data security hardware (such as encryption devices, chips, and circuit boards); passwords, data security software or information (such as test keys and encryption codes); and similar information that is required to access computer programs or data or to otherwise render programs or data into useable forms.

h. Any computer or electronic records, documents, and materials, including those used to facilitate

interstate communications, in whatever form and by whatever means such records, documents, and materials, their drafts or their modifications, may have been created or stored, including, without limitation, any hand-made form (such as writing or marking with any implement on any surface, directly or indirectly, relating to the described offense); any photographic form (such as microfilm, microfiche, prints, slides, negative, video tapes, motions pictures or photocopies); any electrical, magnetic, or electronic form (such as tape recordings, cassettes, compact disks); or any information on an electronic or magnetic storage device (such as floppy diskettes, hard disks, CD-ROMS, optical disks, printer buffers, sort cards, memory calculators, electronic dialers, or electronic notebooks), as well as printouts or readouts from any magnetic storage device.

i. Any electronic information or data, stored in any form, which has been used or prepared for use either for periodic or random backup (whether deliberate, inadvertent, or automatically or manually initiated), of any computer or computer system. The form such information might take includes, but is not limited to, floppy diskettes, fixed hard disks, removable hard disk cartridges, tapes, laser disks, CD-ROM disks, video cassettes, and other media capable of storing magnetic or optical coding.

j. Any electronic storage device capable of collecting, storing, maintaining, retrieving, concealing, transmitting, and using electronic data, in the form of electronic records, documents, and materials, including those used to facilitate interstate communications. Included within this paragraph is any information stored in the form of electronic, magnetic, optical, or other coding on computer media or on media capable of being read by a computer or computer-related equipment, such as fixed disks, external hard disks, removable hard disk cartridges, floppy disk drives and diskettes, tapes drives and tapes, optical storage devices, laser disks, or other memory storage devices.

k. Records of personal and business activities relating to the operation of a computer, such as telephone or modem records, notes (however and wherever written, stored, or maintained), books, diaries, and reference materials relating to the described offense.

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA v. THE PREMISES KNOWN AND DESCRIBED AS THE FIRST FLOOR OF 137-07 FRANKTON STREET, ROSEDALE, NEW YORK 11422	:	**FILED UNDER SEAL** **AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT**

STATE OF NEW YORK)
EASTERN DISTRICT OF NEW YORK) : ss.:

I, CORDEL JAMES, being duly sworn, depose and say:

1. I am a Special Agent with the Federal Bureau of Investigation ("FBI"), assigned to the New York Field Office. I have been in my current position since September 2005. In my current position, I investigate violations of federal criminal laws relating to bank fraud, including violations of 18 U.S.C. § 1029.

2. I have been personally involved in the investigation of this matter. This affidavit is based upon my own knowledge and upon my conversations with other law enforcement agents and my examination of reports and records. Because this affidavit is being submitted for the limited purpose of establishing probable cause, it does not include all the facts that I have learned during the course of my investigation. Where the contents of documents and the actions, statements, and conversations of others are reported herein, they are reported in substance and in part, except where otherwise indicated.

3. For the reasons detailed below, I believe that there is probable cause to believe that CLAUDIA FRANCIS, the defendant, has committed violations of federal law: From at least in or about August 2006, in the Southern District of New York and elsewhere, FRANCIS and others known and unknown, unlawfully, willfully, and knowingly, did combine, conspire, confederate, and agree together and with each other to commit offenses against the United States, to wit, to violate Title 18, United States Code, Section 1029(5). FRANCIS and others known and unknown, unlawfully, willfully, knowingly, and with intent to defraud, did

use credit cards belonging to at least eight other persons to purchase goods and gift cards from retail stores, and on occasion, returned the goods for cash or for credit to her own credit card, receiving money and things of value, the combined value of which exceeded $100,000. FRANCIS was arrested on or about June 28, 2007 upon a complaint sworn and filed in the Southern District of New York, White Plains, on June 27, 2007 (attached hereto as Exhibit A) at her residence located at 137-07 Frankton Street, Rosedale, New York 11422 ("PREMISES"). At the time of her arrest, there was in plain view shredded credit cards and approximately 50 gift cards. Also found upon a search of the house incident to arrest, the agents found were two safes with model numbers (one safe on the bed in CLAUDIA FRANCIS' room and one in a closet), two computers, flat screen plasma televisions, electronic equipment such as DVD recorders and cam corders located throughout the house as described further below. I further believe that there will be found additional evidence, fruits, and instrumentalities of the offense for which FRANCIS is charged, as described in Attachment A to the Affidavit.

4. Further, based on my personal observations and my conversations with other law enforcement officers, I know that:

a. The PREMISES is a private home located at 137-07 Frankton Street, Rosedale, New York 11422, which is a building located in Rosedaul, New York.

b. The PREMISES is a two story multiple family house, with a basement. The first floor is made out of a brown brick; the second floor has green shingles. The house has multiple windows. There is a driveway that runs from the street, along the side of the house, to the back yard. There is no garage. There are two front doors made of a solid light wood, with black trim. The number "137" appears between the two doors, with "07" below it. There is a pathway which leads to stairs to the front door. FRANCIS lives on the first floor.

c. When agents arrived at the house, there were two cars parked in the driveway. One of those cars is a Honda Accord with New York license plats, number "DFH 1510". According to New York's Department of Motor Vehicles ("DMV"), this car belongs to FRANCIS. New York's DMV also lists the PREMISES as FRANCIS' address.

d. When FRANCIS was arrested, two children were

present in the house. The brother-in-law, in another apartment in the same building, drove the children away in the other car.

5. When FBI agents arrived at the PREMISES, they did a sweep of the house and saw in plain a shredder containing shredded credit cards and/or gift cards, approximately 50 gift cards, and one Cingular reward debit card located in the house as follows:

a. On the floor of the living room, there was a clear plastic shredder (with an opaque top) that was half filled with what appeared to be shredded credit cards and/or gift cards. There were approximately 20 cards on a table in the living room.

b. In a bedroom in the back of the house, where CLAUDIA FRANCIS was sleeping, there were approximately 20 gift cards on a dresser.

c. In the kitchen there were 4 gift cards on a table.

d. There were a couple of gift cards and the Cingular reward debit card in the dining room on a table.

6. In addition, there were two safes, three computers, two laptops, at least five flat screen televisions, DVD recorders, an X-Box 360 and Playstaion in the house, as well as numerous videos. Both safes were in the bedroom; one of the safe's was a Century 1100 model; the other was a Century 1330 model. The computers and laptop were located as follows and had the serial numbers set forth below:

a. In the living room there were: (i) an HP Computer Pavillion with Serial Number MXX7130852; and (ii) an HP Office Jet Pro Scanner Printer with Serial Number MY71B120M9 (the computer and printer were approximately one foot away from where the shredder and gift cards were located in the living room);

b. In a bedroom in the back of the house, where CLAUDIA FRANCIS was sleeping there was an HP Pavilion Laptop with Serial Number 2CE712251R;

c. In a room that appeared to be that of CLAUDIA FRANCIS' sons, there were: (i) a Compaq Laptop

Serial Number 1V1BKDKN3648; (ii) a Compaq Presario Computer with Serial Number CNC33909V3;

d. In a room that appeared to be that of CLAUDIA FRANCIS' daughter, there was a Compaq Presario Computer with Serial Number MXK33813Z1.

THE INVESTIGATION

7. In or about November 2006, Nordstrom contacted the FBI to inform the FBI that they believed that members and associates of the FRANCIS family were purchasing goods on other persons' credit cards and returning the goods for credit to their own credit cards. Following a meeting with a Loss Prevention Manager at Nordstrom, and a review of documents and records from and numerous banks, including Citibank, Commerce Bank, PNC Bank, Municipal Credit Union, Bank of America, and Wachovia Bank NA, as well as interviews of a number of the true holders of the credit cards, I learned the following:

a. On August 22, 2006, the credit card of an individual identified herein as Victim 1 was used to purchase goods in the amounts of $1,122.10 and $502.44 at two Nordstrom stores, one in Garden City, New York, the other in Westbury, New York. Victim 1 has confirmed with the credit card company that the transactions were unauthorized. The retail store's records show that some of the goods purchased on August 22, 2006 for the total amount of $1,122.10 were returned to the same store for credit to a different credit card in the amounts $874.43 and $247.67 on August 25 and 28, 2006 respectively. These two amounts appear as credits on August 25 and 28, 2006 in the bank account for the credit card belonging to CLAUDIA FRANCIS. Further, the retail store's records show that some of the goods purchased on August 22, 2006 for the total amount of $502.44 were returned to the same store for credit to a different credit card in the amounts of $104.59 and $104.59 (that is, the same amount credited twice) on September 5, 2006. This amount appears twice as credits on September 5, 2006 in the bank account for the credit card belonging to CLAUDIA FRANCIS.

b. On April 17, 2007, the credit card of an individual identified herein as Victim 2 was used

to purchase goods in the amount of $299.99 at a retail store in Valley Stream, New York. I have spoken to Victim 2 and Victim 2 has confirmed that this transaction was unauthorized. The goods were returned to the same store on April 19, 2007, and a gift card was received in exchange. The gift card was then used on the same day to purchase different goods which required installation in a car. The installation, in turn, required the customer to sign a "workorder" form. The name signed and address given on the workorder were those of CLAUDIA FRANCIS.

c. The credit card of Victim 1 was also used to purchase goods at Nordstrom stores, which goods were returned to Nordstrom stores for credit to credit cards belonging to JHAMEL SEAN FRANCIS and KENNETH FRANCIS as follows:

i. On August 22, 2006, the credit card of Victim 1 was used to purchase goods in the amount of $322.14 a retail store located in White Plains, New York. Victim 1 has confirmed with the credit card company that this transactions was unauthorized. On September 19, 2006, the goods were returned to another store in the same retail chain for two credits in the amounts of $108.55 and $213.59. These two amounts appear as credits on September 19, 2006 in the bank account for the credit card belonging to JHAMEL SEAN FRANCIS.

ii. On August 22, 2006, the credit card of Victim 1 was used to purchase goods in the amounts of $749.73 and $972.19 at two stores in the same retail chain, one in White Plains, New York and the other in Garden City, New York. Victim 1 has confirmed with the credit card company that these transactions were unauthorized. On September 16, 2006, these goods were returned to two different stores in the same retail chain for credit to a different credit card in the amounts of $749.73 and $972.19. These two amounts appear as credits on September 16, 2006 in the bank account for the credit card belonging to KENNETH FRANCIS.

d. According to Citibank records, the credit card of Victim 1 was used to make at least $7,000.00 worth of unauthorized purchases.

e. In addition to these unauthorized transactions, there have been numerous other unauthorized transactions effected by persons associated with CLAUDIA FRANCIS. As set forth in the attached complaint, the credit cards belomging to at least eight victims, including Victims 1 and 2, have been used to purchase goods that were returned for cash or credit to the accounts of the defendants named in the complaint. The compromised credit cards were used to effect unauthorized transactions worth more than $100,000.

f. The Postal Carrier for the address 137-07 Frankton Street, Rosedale, New York 11422 has stated that CLAUDIA FRANCIS receives mail at this address. As noted above, this address is also the address for CLAUDIA FRANCIS in the DMV's records.

PROBABLE CAUSE

8. Based on the foregoing, I believe there is probable cause to believe that the electronic equipment found at the PREMISES, including the flat screen plasma televisions, the computers and laptops, the electronic game equipment, was purchased with credit cards belonging to other persons.

9. Based on the foregoing, I believe there is probable cause to believe that, in addition to the items listed above, there are documents, physical items, materials, and records relating to the conspiracy charged in the Complaint at the PREMISES.

10. Based on my training and experience, and my conversations with other law enforcement officers who have experience with schemes to defraud by the use of access devices belonging to other persons, I believe that the two safes at the PREMISES contain fruits of the offense for which CLAUDIA FRANCIS has been charged.

11 Based on my training and experience, and my conversations with other law enforcement officers who have experience with schemes to defraud by the use of access devices belonging to other persons, I believe that the computer at the

PREMISES is also likely to be a storage device for evidence of the crime because computers often maintain data directly on the hard drive, including documents and electronic mail messages that have been deleted by the user, but have not yet been overwritten by new files by the computer, and therefore remain potentially recoverable. Based on my conversations with other agents who have experience with the use of computers in criminal activity, I also have learned that CD-ROMs, hard disks, floppy disks, together with peripheral equipment such as keyboards, printers, modems or acoustic couplers, and magnetic tapes, can to be as a storage device for evidence of the crime.

12. Based on training and experience, and conversations with other law enforcement officers who have experience with computer crimes, I have also learned the following:

a. Persons who use a computer system inside a residence generally leave items, such as letters, papers, notes, and other documents and information, in their residences that may assist in identifying the person or persons who uses that computer system, and in identifying any user names or passwords needed to operate the computer. While such items are normally located near the computer system, they can be found anywhere inside the residence; and

b. Computer systems located inside a residence generally contain files and data, such as letters, documents, e-mail, etc., that can be used to identify the person or persons who use that computer system, and in identifying any user names or passwords needed to operate the computer. As files and data that can be used to identify the person or persons using the computer system come in an infinite variety of formats and types, this Affidavit requests authorization to search all files and data contained in any computer system found within the PREMISES.

13. Based on the foregoing, I seek permission to seize any item, in whatever format, including digital—more particularly described in Attachment A—inside the PREMISES and/or stored on a computer system inside the PREMISES.

Methods To Be Used To Search Computers

14. Based on my training, my experience, and my conversations with other law enforcement agents, I have learned that searching for computerized information for evidence or instrumentalities of a crime commonly requires agents to seize most or all of a computer system's input/output peripheral devices, related software documentation, and data security devices (including passwords) so that a qualified computer expert can accurately retrieve the system's data in a laboratory of other controlled environment. This is true for the following reasons:

a. The volume of evidence. Computer storage devices (such as hard disks, diskettes, compact disks, tapes, etc.) can store the equivalent of thousands of pages of information. In addition, a user may seek to conceal evidence of criminal activity by storing it in random order with deceptive file names. Searching authorities are thus required to examine all the stored data to determine which particular files are evidence or instrumentalities of criminal activity. This sorting process can take weeks or months, depending upon the volume of data stored, and it would be impractical to attempt this kind of data analysis "on-site."

b. Technical requirements. Analyzing computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications. Thus, it is difficult to know prior to the search which expert possesses sufficient specialized skills to best analyze the system and its data. No matter which system is used, however, data analysis protocols are exacting scientific procedures, designed to protect the integrity of the evidence and to recover even "hidden," erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (both from external sources or from destructive codes embedded in the system as a "booby trap"), a controlled environment is essential to its complete and accurate analysis. Accordingly, as stated above, it is usually necessary that the above-referenced equipment, software, data, and related

instructions be seized and subsequently processed by a qualified computer specialist in a laboratory setting. It may be the case, however, under appropriate circumstances, that some types of computer equipment can be more readily analyzed and pertinent data seized on-site, thus eliminating the need for its removal from the premises.

15. The analysis of electronically stored data will be performed at a FDA-OCI, or a place that the FDA-OCI sends the information to for analysis, and may entail any or all of several different techniques. Such techniques may include, but shall not be limited to, surveying various file "directories" and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files); "opening" or reading the first few "pages" of such files in order to determine their precise contents; "scanning" storage areas to discover and possibly recover recently deleted data; scanning storage areas for deliberately hidden files; and performing electronic "key-word" searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are related to the subject matter of the investigation.

16. If, after inspecting the input/output peripheral devices, system software, and pertinent computer related documentation, it becomes apparent that these items are no longer necessary to retrieve and preserve the evidence, such materials and/or equipment will be returned within a reasonable time, unless the Government obtains the Court's permission to continue to keep the property seized during the execution of the search warrant.

17. It may be necessary for programmers and other outside experts to assist the FBI during the examination of the computer evidence in order to help identify ownership and trace the theft of the source code and the e-mail relating to it.

CONCLUSION

WHEREFORE, I respectfully request that a warrant be issued authorizing FBI agents and officers, and computer technicians employed by the FBI, with proper assistance from other law enforcement officers, to enter the PREMISES and search for and seize the items as set forth in Attachment A according to the procedures described herein.

CORDEL JAMES
Special Agent
Federal Bureau of
Investigation

Sworn to before me this
28th day of June, 2007

UNITED STATES MAGISTRATE JUDGE
EASTERN DISTRICT OF NEW YORK

ATTACHMENT A

PROPERTY TO BE LOCATED AND SEIZED WITHIN THE PREMISES KNOWN AND DESCRIBED AS AT 137-07 FRANKTON STREET, ROSEDALE, NEW YORK 11422

a. The three computers, a scanner printer Copy and two laptops identified as follows:

i. an HP Computer Pavillion with Serial Number MXX7130852;

ii. an HP Office Jet Pro Scanner Printer with Serial Number MY71B20M9;

iii. In a bedroom in the back of the house, where CLAUDIA FRANCIS was sleeping there was an HP Pavilion Laptop with Serial Number 2CD712251R;

iv. In a room that appeared to be that of CLAUDIA FRANCIS' sons, there were: (i) a Compaq Laptop Serial Number 1V1BKDKN3648; (ii) a Compaq Presario Computer with Serial Number CNC33909V3;

v. In a room that appeared to be that of CLAUDIA FRANCIS' daughter, there was a Compaq Presario Computer with Serial Number MXQ03381321.

b. The two safes, one a Century 1100 Model and one a Century 1330 model, and the contents thereof after opening;

c. The televisions and other electronic equipment such as DVD recorders, printers, camcorders, Playstation, X-box 360 and videos.

d. Computer hardware, meaning any and all computer equipment including all electronic devices which are capable of collecting, analyzing, creating, displaying, converting, storing, concealing, or transmitting electronic, magnetic, optical, or similar computer impulses or data. Included within the definition of computer hardware is any data processing hardware (such as central processing units and self-contained laptops or notebook computers), internal or peripheral storage

devices (such as fixed disks, external hard disks, floppy disk drives, and diskettes, tape drives and tapes, optical and compact disk storage devices, and other memory storage devices); peripheral input/output devices (such as keyboards, printers, scanners, plotters, video display monitors, and optical readers); related communications devices (such as modems, cables and connections, recording equipment, RAM and ROM units, acoustic couplers, automatic dialers, speed dialers, programmable telephone dialing or signaling devices, and electronic tone generating devices); and any devices, mechanisms, or parts that can be used to restrict access to such hardware (such as physical keys and locks);

e. Computer software, meaning any and all information, instructions, programs, or program codes, stored in the form of electronic, magnetic, optical, or other media, which is capable of being interpreted by a computer or its related components. Computer software may also include data, data fragments, or control characters integral to the operation of computer software, such as operating systems software, applications software, utility programs, compilers, interpreters, communications software, and other programming used or intended to be used to communicate with computer components.

f. Computer-related documentation, meaning any written, recorded, printed, or electronically-stored material which explains or illustrates the configuration or use of any seized computer hardware, software, or related items.

g. Computer passwords and data security devices, meaning any devices, programs, or date - whether themselves in the nature of hardware or software - that can be used or are designed to be used to restrict access to, or to facilitate concealment of, any computer hardware, computer software, computer-related documentation, or electronic data records. Such items include, without limitation, data security hardware (such as encryption devices, chips, and circuit boards); passwords, data security software or information (such as test keys and encryption codes); and similar information that is required to access computer programs or data or to otherwise render programs or data into useable forms.

h. Any computer or electronic records, documents, and materials, including those used to facilitate

interstate communications, in whatever form and by whatever means such records, documents, and materials, their drafts or their modifications, may have been created or stored, including, without limitation, any hand-made form (such as writing or marking with any implement on any surface, directly or indirectly, relating to the described offense); any photographic form (such as microfilm, microfiche, prints, slides, negative, video tapes, motions pictures or photocopies); any electrical, magnetic, or electronic form (such as tape recordings, cassettes, compact disks); or any information on an electronic or magnetic storage device (such as floppy diskettes, hard disks, CD-ROMS, optical disks, printer buffers, sort cards, memory calculators, electronic dialers, or electronic notebooks), as well as printouts or readouts from any magnetic storage device.

i. Any electronic information or data, stored in any form, which has been used or prepared for use either for periodic or random backup (whether deliberate, inadvertent, or automatically or manually initiated), of any computer or computer system. The form such information might take includes, but is not limited to, floppy diskettes, fixed hard disks, removable hard disk cartridges, tapes, laser disks, CD-ROM disks, video cassettes, and other media capable of storing magnetic or optical coding.

j. Any electronic storage device capable of collecting, storing, maintaining, retrieving, concealing, transmitting, and using electronic data, in the form of electronic records, documents, and materials, including those used to facilitate interstate communications. Included within this paragraph is any information stored in the form of electronic, magnetic, optical, or other coding on computer media or on media capable of being read by a computer or computer-related equipment, such as fixed disks, external hard disks, removable hard disk cartridges, floppy disk drives and diskettes, tapes drives and tapes, optical storage devices, laser disks, or other memory storage devices.

k. Records of personal and business activities relating to the operation of a computer, such as telephone or modem records, notes (however and wherever written, stored, or maintained), books, diaries, and reference materials relating to the described offense.